Security and Privacy in Car2Car Adhoc Networks

Antonio Kung

Trialog

www.trialog.com

Introduction

- French SME
- Involved since 2002 in security and privacy for connected vehicles

Outline

- Background
- Integration of Security and Privacy
  - Adhoc network viewpoint
    - Experience from ISE project
  - Connected vehicle viewpoint
    - Privacy: Experience from PRIPARE project
    - Big data: Experience from AUTOMAT project
- Conclusion

Security and Privacy Issues

- Security
  - A car is connected and therefore can be hacked
  - A car is part of the Internet of things
  - A car is a system within systems
- Privacy
  - A car is connected and therefore can be tracked
  - A car can collect data
    - IoT, Big data, Cloud

Car-2-Car Infrastructure

- Adhoc Networks
  - V2V: Vehicle-to-Vehicle
  - V2I: Vehicle-to-Infrastructure (RSU: Road Side Unit)
- Type of communication
  - ETSI TC ITS
    - ITS G5
    - allocated spectrum (5,85 – 5,925 Ghz)
  - IEEE 802.11p link
- Type of messages
  - Broadcast/Geocast

Types of Messages

- CAM: Cooperative Awareness Messages
  - Vehicle dynamics info
    - Position,
    - Speed,
    - Heading
    - …
- DENM: Decentralized Environmental Notification Messages
  - Information on dynamic environment
    - Accident ahead,
    - Traffic jam ahead
    - …

Some Research Projects in Europe

SEVECOM

Secure Vehicle Communication 2008

PRECISA

ITS Privacy 2011

evita

In-Vehicle Security 2011

PRIPARE

Privacy-by-design 2016

AutoMat

Vehicle Big Data 2017

PRESERVE
preparing secure v2x communication systems

Solution for field operational tests 2014

ISE
ITS Security

Validate Deployment 2017

Initial Decisions (SEVECOM Project)

- Authenticity and Integrity
  - Use signatures
  - 1000 verifications per second
    - PRESERVE and C2C-CC specifications
- Avoid tracking / No fixed address
  - Use pseudonyms certificates (PC)
    - Short-term certificates
    - Changed according to **policies**

References today

- US Secure Message and Certificate Format
  - IEEE 1609.2
- US Cryptography
  - IEEE 1609.3

- Reference Architecture
  - ETSI TS 102 940
- Trust and Privacy Management (enrollment and PKI)
  - ETSI TS 102 941
- Certificate Format
  - ETSI TS 103 097
- CAM Format
  - ETSI EN 302 637-2
- DENM Format
  - ETSI EN 302 637-3

- MoU (2011)
- Protection Profiles

Outline

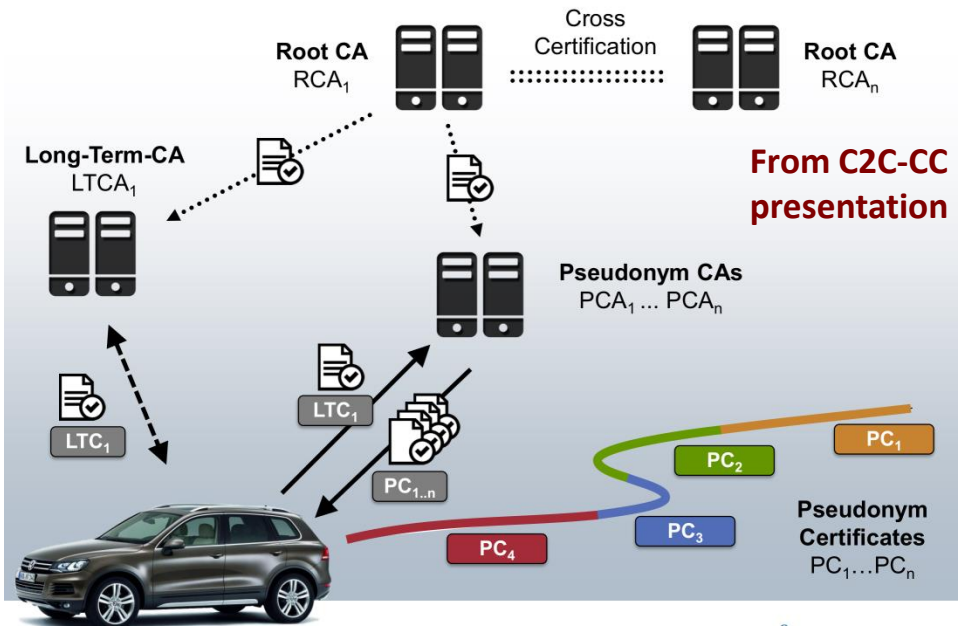
- Background
- Integration of Security and Privacy
  - Adhoc network viewpoint
    - Experience from ISE project
  - Connected vehicle viewpoint
    - Privacy: Experience from PRIPARE project (Privacy)
    - Big data: Experience from AUTOMAT project
- Conclusion

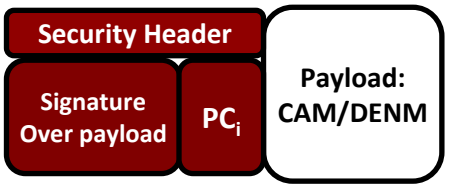
ISE Project

- ITS **SE**curity
  - Part of SystemX
    - Technology Research Institute)
    - Member ETSI and Car2Car consortium
  - http://www.irt-systemx.fr/en/project/ise/
- ISE Objectives
  - Cost effective C-ITS security system
  - Integrates infrastructure PKI
  - Methods and tools for assurance and trust
- Cooperation with C-ITS pilot (SCOOP@F part 2)
  - https://ec.europa.eu/inea/en/connecting-europe-facility/cef-transport/projects-by-country/multi-country/2014-eu-ta-0669-s

Example of Public Key Infrastructure

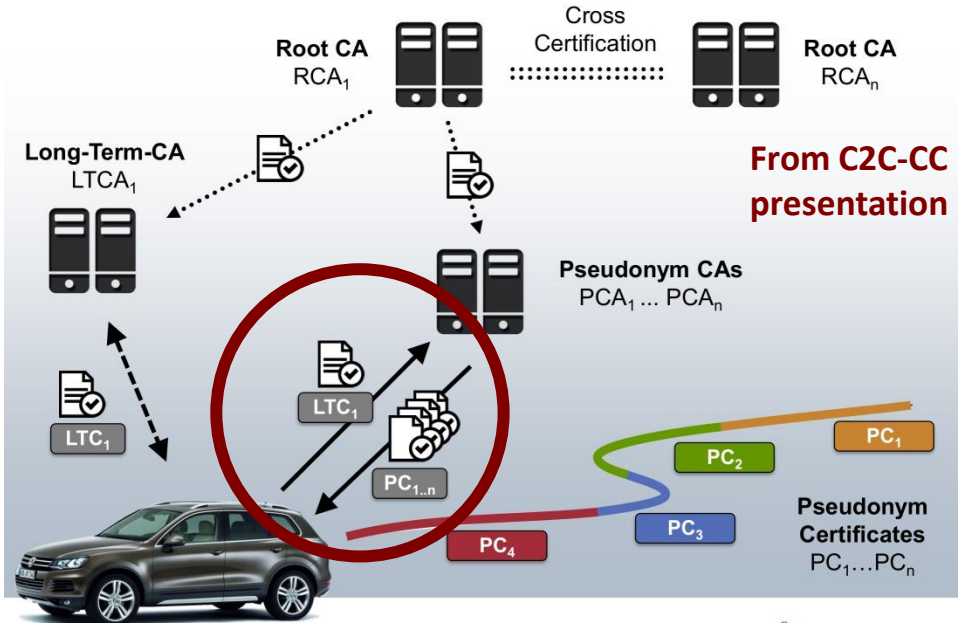
- Purpose: management of pseudonyms certificates
- Enables
  - Authentication & authorization of senders
  - Integrity: receivers verify data via digital signatures
- Certificate Authority Structure
  - Root CA
  - Long term CA
    - Register vehicle
  - Pseudonym CA
    - Provides pseudonyms

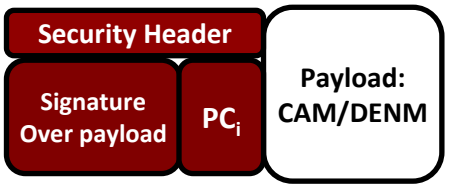




How Pseudonym Certificates Work

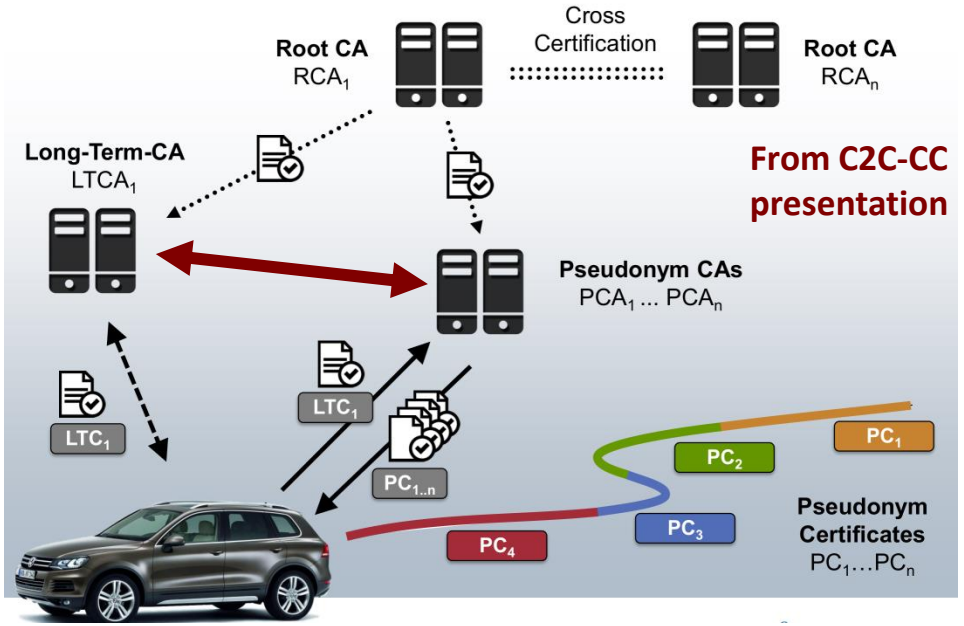
- Vehicles and Road side units receive certificates from PCA
- Pseudonym certificates frequently changed
- Secure communications between nodes
  - Vehicle and RSU
  - CAs





Extension proposed by ISE for Privacy

- Request for pseudonyms to PCA
  - One pseudonym per request only!
    - PCA cannot link pseudonyms
  - Authentication of vehicles during request by LTCA only
    - PCA cannot identify vehicles
    - Part of request is encrypted and only readable by LTCA



Issues

- Organisational
  - PKI deployment
- Operational
  - Pseudonym change policy
  - Revocation
  - Maintainability of crypto
  - Assurance
  - Integrating security with safety

PKI Deployment

- Governance
  - who is in charge?
    - European PKI?
    - National PKIs?
    - Car Manufacturer PKI?
    - Road operators PKI?
  - Root CAs?
    - Cross-certification issues?
    - Usage of Trusted-service Status List (TSL) including Root CAs and PCAs certificates?
- Protocol with PKI not standardized

Pseudonym Change Policy

- Find the suitable policy?
  - Change at startup, periodic change?
    - Need for standardization
  - Communication stack “agility” issue
    - Implementation still using previous pseudonym
    - Node may blocked a while before being able to transmit
- Conflicts of interest between stakeholders
  - Road operators
    - Needs to track vehicles for a while (traffic monitoring)
    - e.g. 1 pseudonym change every 2 hours)
  - Data protection authorities
    - Each message has a different pseudonym

Revocation of Pseudonym

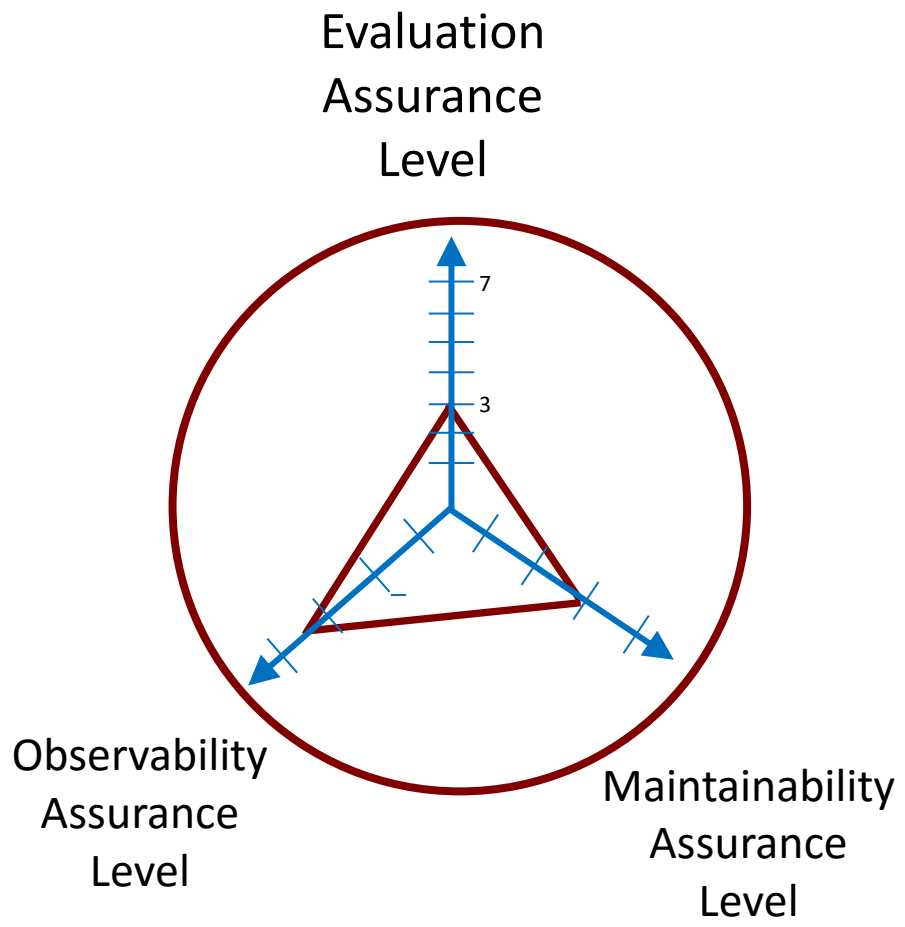
- Revoking certificates
  - Retirement
  - Car stolen
  - …
- Typical approach
  - Use Certificate Revocation List (CRL)
- Issues
  - Millions of vehicles
    - CRLs need to be distributed to every vehicle?
    - Real-time updates?
    - Regional CRLs?

Maintainability of Crypto

- Need to change encryption algorithms in case of security issue
- Maintainability
  - How to update V2X stack with new algorithms/parameters?
- Interoperability
  - e.g. ETSI standard contains placeholders for extension
  - But operational process is not decided yet

Assurance

- Common Criteria too costly
  - Focus on evaluation assurance mainly
  - Issues
    - Cost
    - Need to integrate in automotive engineering process
    - System of systems
    - Product evolutions
- ISE multidimensional types of assurance
  - Evaluation + Maintainability + Observability assurance level = Overall Trust assurance level?

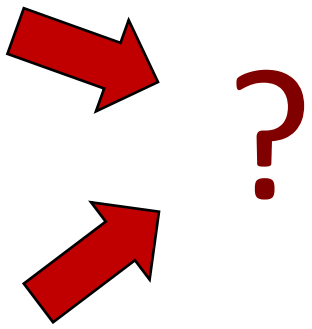


Integrating Security with Safety

- Merge safety risk analysis and security risk analysis
- Integrate Security-by-design in automotive design process
  - SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
  - Proposal for ISO standard: Automotive Security Engineering TC22

ASIL Automotive Safety Integration Level

Automotive Trust Integration Level?



Outline

- Background
- Integration of Security and Privacy
  - Adhoc network viewpoint
    - Experience from ISE project
  - Connected vehicle viewpoint
    - Privacy: Experience from PRIPARE project (Privacy)
    - Big data: Experience from AUTOMAT project
- Conclusion

PRIPARE Project

- **PR**eparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **Re**search
  - http://pripareproject.eu/
- Methodology Handbook for Privacy-by-design
  - Lifecycle oriented
  - Proposal for ISO standard: Privacy Engineering (ISO SC27)

Funded by the European Commission (FP7)

TRIALOG
Atos
Gradiant
CENTRO TECNOLÓXICO DE TELECOMUNICACIÓNS DE GALICIA
Trilateral Research & Consulting
Inria
INVENTEURS DU MONDE NUMÉRIQUE
POLITÉCNICA
"Ingeniamos el futuro"
THE AMERICAN UNIVERSITY of PARIS 50 YEARS
KU LEUVEN
Fraunhofer
ulm university universität uulm

GDPR: General Data Protection Regulation

European Regulation
Enter into force on May 24th 2016
Fully applied on May 25th 2018

- Privacy-by-design (PbD) and by-default
- Privacy Impact Assessment (PIA)
- Data Protection Officers
  - All public authorities and companies processing personal data on a large scale
- Sanctions for breaches
  - up to 20,000,000 EUR
  - up to 4% of the annual worldwide turnover

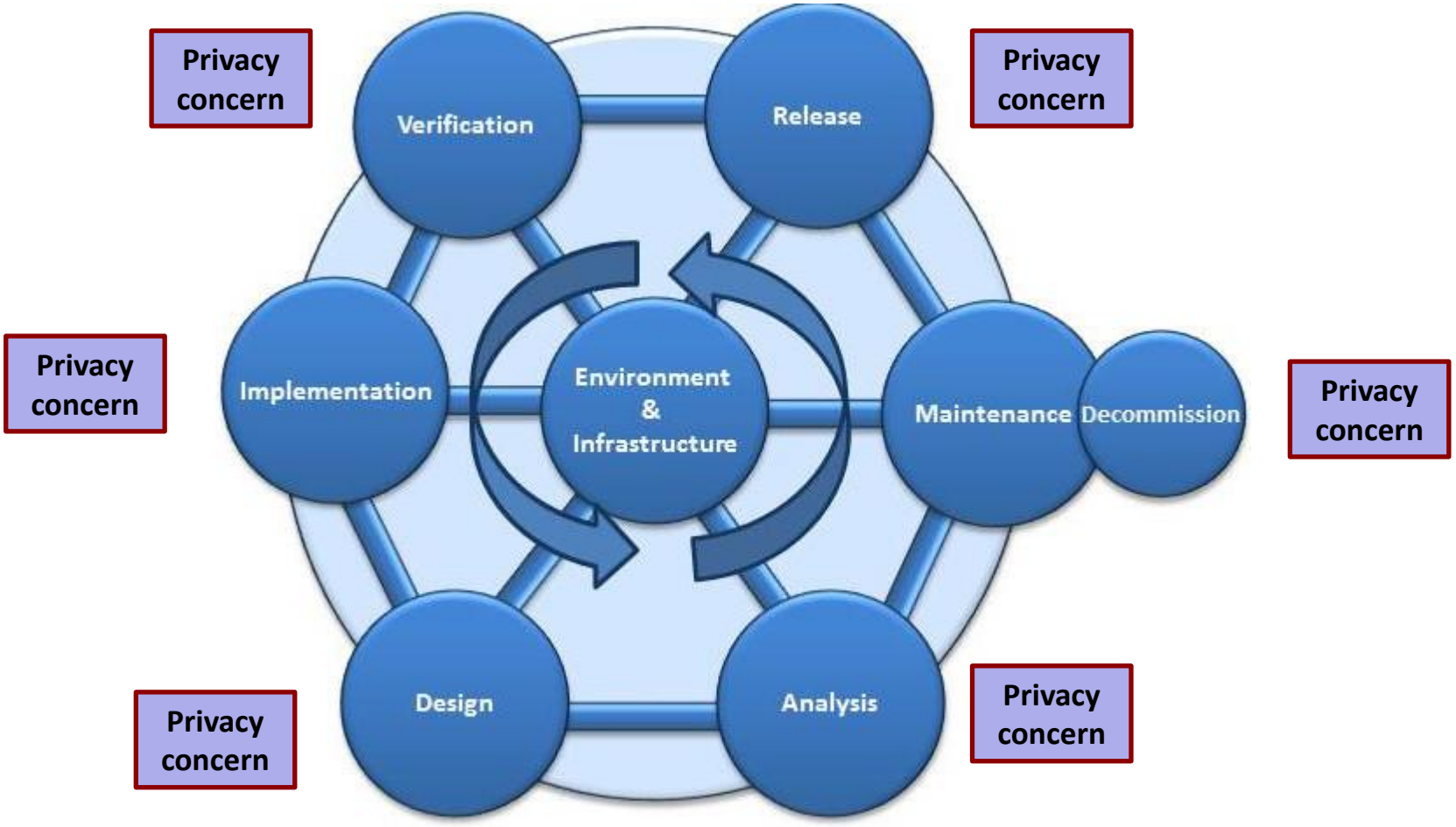
Issues

- Integrating Privacy Management in Supply Chain
- Integrating Privacy Management in Lifecycle
- New types of threats
- New properties

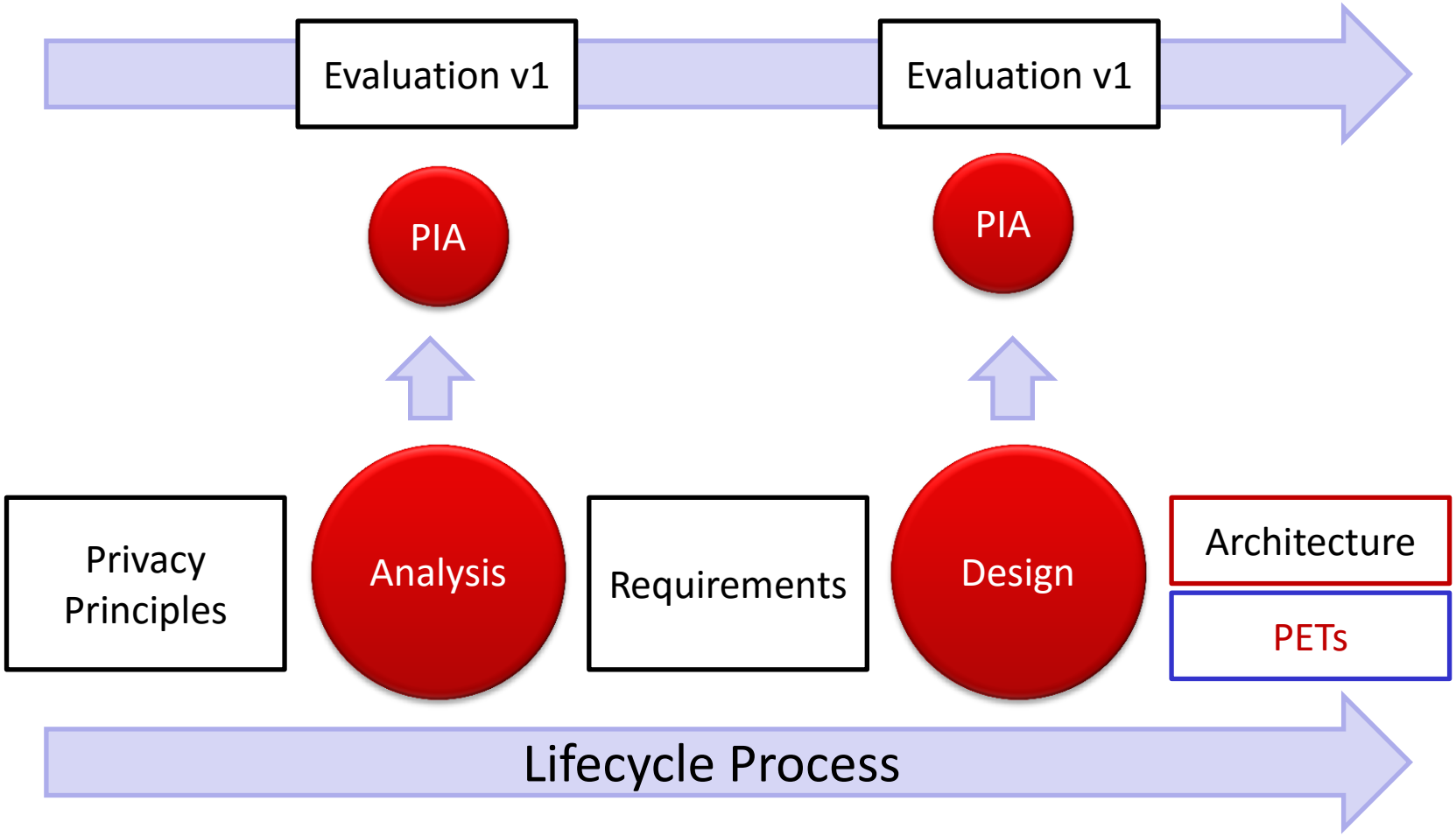
Several Types of Concerns

Stakeholder		Legal Compliance Level	Management Level	System Lifecycle Level
Demand side	Policy maker 	**e.g. Compliance Check**		
	Operator Data Controller 	Regulation **GDPR**	Privacy Impact Assessment **PIA**	Privacy-by-Design **PbD**
	Operator Data processor 			
Supply side	**Supplier** 	**e.g. Operators Requirements**		

Integrating privacy-by-design



A Glimpse on the Process



STRIDE Security Threats Analysis

Property	Description	Threat
Authentication	The identity of users is established (or you're willing to accept anonymous users).	**S**poofing
Integrity	Data and system resources are only changed in appropriate ways by appropriate people.	**T**ampering
Nonrepudiation	Users can't perform an action and later deny performing it.	**R**epudiation
Confidentiality	Data is only available to the people intended to access it.	**I**nformation disclosure
Availability	Systems are ready when needed and perform acceptably.	**D**enial Of Service
Authorization	Users are explicitly allowed or denied access to resources.	**E**levation of privilege

LINDDUN Privacy Threats Analysis

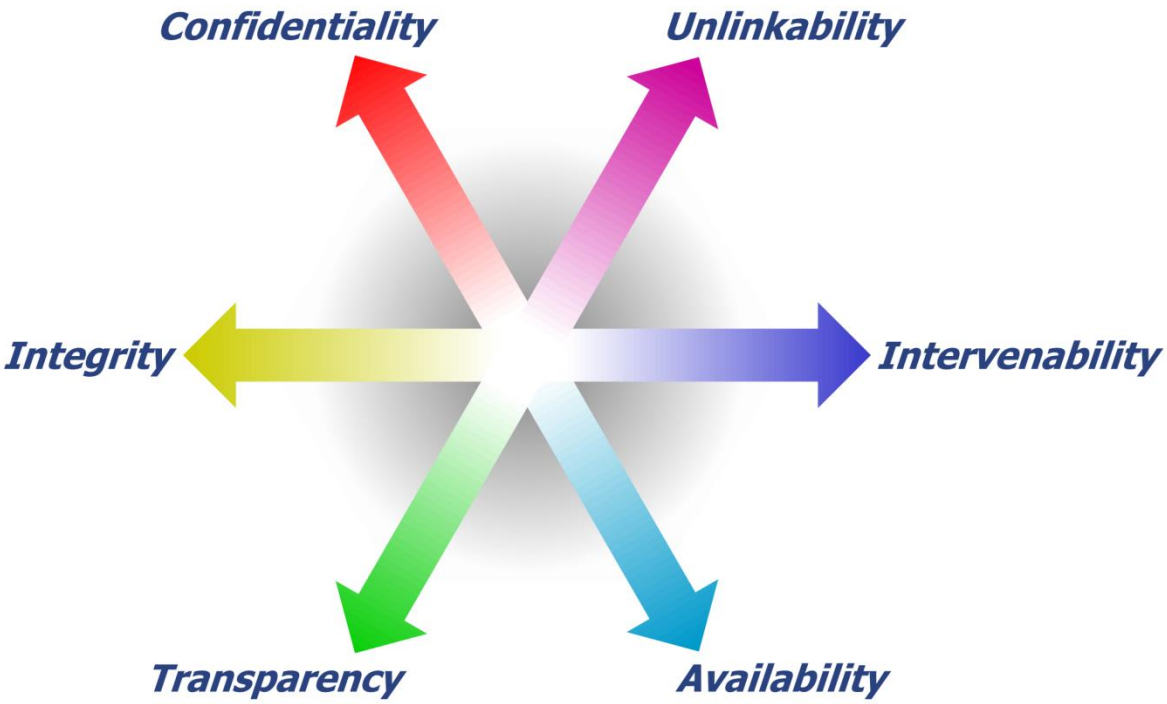
Type	Property	Description	Threat
Hard privacy	Unlinkability	Hiding the link between two or more actions, identities, and pieces of information.	**L**inkability
	Anonymity	Hiding the link between an identity and an action or a piece of information	**I**dentifiability
	Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict	**N**on-repudiation
	Undetectability and unobservability	Hiding the user's actvities	**D**etectability
Security	Confidentiality	Hiding the data content or controlled release of data content	**D**isclosure of information
Soft Privacy	Content awareness	User's consciousness regarding his own data	**U**nawareness
	Policy and consent compliance	Data controller to inform the data subject about the system's privacy policy, or allow the data subject to specify consents in compliance with legislation	**N**on compliance

https://distrinet.cs.kuleuven.be/software/linddun/catalog.php

Beyond CIA

- Confidentiality
- Integrity
- Availability

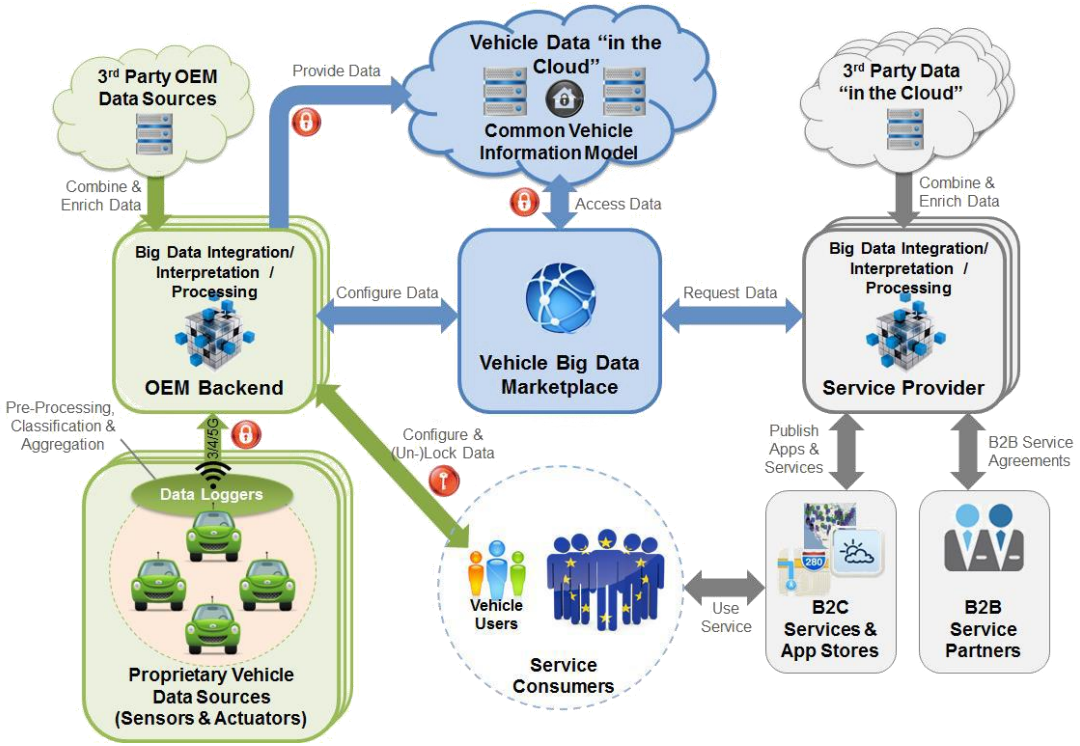
- Unlinkability
- Intervenability
- Transparency



From ULD: ieee-security.org/TC/SPW2015/IWPE/2.pdf

Vehicle Big Data Marketplace

- http://www.automat-project.eu/



Funded by the European Commission (H2020)

Some Considerations in AUTOMAT

- Using anonymized vehicle data in other cross-sectorial contexts
  - Socially beneficial services
  - Economically relevant services
- Protecting customer's legitimate privacy
- Example of scenario
  - Data collected only upon customer consent
  - Data managed by customer (switch of paradigm from CRM to VRM – Vendor Relationship Management)

Conclusion

- Cybersecurity for connected vehicles: a system of system practice in the making
  - Integrate security-by-design
  - Integrate privacy-by-design

- New projet in France
  - CTI: Cybersecurity in Intelligent Transport
    - Combines automotive, aeronautic and railway domains
  - Objective: Guidelines on cybersecurity for ITS
    - Risk analysis
    - Assurance process
    - Merging security and safety


SMART GRID
& METERING


E-MOBILITY


HEALTH & SOCIAL


CYBER SECURITY
& PRIVACY

Thanks